ZSCALER COVER LETTER TO DPA

Thank you for choosing Zscaler as your cloud security provider. Before you review our Data Processing Agreement (DPA), we wanted to highlight the following key points about Zscaler which should assist you in your review:

1. Since Zscaler is a multi-tenant, security-as-a-service provider, we must maintain consistent data privacy and security controls and procedures across the thousands of customers on our cloud as much as possible. We have certified to the ISO 27001 information security framework to maintain consistent and robust security controls and procedures for all customers. Zscaler also adheres to System and Organization Controls (SOC) 2, Type II standards. These certifications and reports can be provided to you upon request and our CISO Team would be happy to walk your security team through our security controls and procedures. Additional information is available at: www.zscaler.com/company/compliance.

2. Data privacy and security are at the core of Zscaler's business and something Zscaler takes very seriously. Zscaler remains committed to protecting personal data in compliance with the highest standards. More information on Zscaler's data privacy compliance efforts is available at: https://www.zscaler.com/products/data-protection-and-privacy.

3. Zscaler has incorporated the appropriate Standard Contractual Clauses into this DPA to govern any transfers of personal data from the European Union, the United Kingdom, and/or Switzerland to a country or recipient that is not providing an adequate level of protection.

4. As opposed to most other SaaS vendors that you may use, Zscaler processes and stores a limited amount of customer data (e.g., IP addresses, URLs, user IDs, user groups, and departments from corporate directory) and do not require the processing of sensitive data (e.g., health data, credit card data, etc.). For the majority of Zscaler's services and products, HTTP, HTTPS, and non-HTTP transaction content is never stored by Zscaler or written to disk - all inspection takes place in memory. If you are ordering our cloud sandbox product, Zscaler records malicious content to a storage disk; however, you can decide what files to send to Zscaler's sandbox (based on file type, URL category, user/group, etc.). You can also obfuscate your user IDs from ever being seen by Zscaler Operations and Support teams or your own administrators. Enabling SSL inspection does not change the limited amount of data that Zscaler processes or stores, instead it provides an added layer of security protection for those threats concealed behind encrypted traffic. It therefore provides additional protection for our customers' employees and other users.

5. As our services follow users throughout the globe, Zscaler processes customer data (which may include personal data) around the globe at its network of 100+ data centers. Zscaler will process customer data at its closest data center(s) to where your users are located (i.e. EU data centers for EU users, U.S. data centers for U.S. users, etc.). For example, in the event an EU user travels to the United States, then Zscaler would process customer data from its closest U.S. data center. Zscaler also provides global support services from the U.S., EU, India, and Costa Rica in order to ensure 24x7x365 coverage.

6. Transaction logs, and the indexes thereof, are stored on separate systems, with separate logical and security controls, for rolling six (6) month periods to ensure a seamless experience.   An individual user cannot be identified without Zscaler's user interface bringing together information from the transaction logs and information from the CA. In addition, no matter where your users are located globally, Zscaler gives you the option at deployment of storing your transaction logs exclusively in (1) the EEA and Switzerland for ZIA and (ii) the EEA for ZPA.

[NOTE: THIS COVER LETTER MAY BE DELETED AFTER READING AND PRIOR TO REDLINING THE DPA